



JETNR

Journal of Emerging Trends and Novel Research

JETNR.ORG | ISSN : 2984-9276

An International Open Access, Peer-reviewed, Refereed Journal

QUANTUM CRYPTOGRAPHY FOR FUTURE SECURITY: PRINCIPLES, STANDARDS, AND THE PATH TO A QUANTUM-SAFE WORLD

1Prof. Roshni Patel, 2Nitin Kumar, 3Vegda Harsh, 4Prisha Bhat

1Supervisor & Faculty, Department of Information Technology

2,3,4Undergraduate Students, Department of Information Technology

Department of Information Technology, Undergraduate Program, 2025

Abstract — The emergence of quantum computing represents a fundamental disruption to the cryptographic foundations upon which modern digital communications depend. Classical asymmetric encryption systems, including RSA and Elliptic Curve Cryptography (ECC), derive their security guarantees from mathematical problems that quantum algorithms can solve in polynomial time. The practical realization of fault-tolerant quantum computers—now regarded by leading researchers as an engineering challenge rather than a theoretical question—places the global security infrastructure in urgent jeopardy. Compounding this threat, the Harvest Now, Decrypt Later (HNDL) attack strategy allows adversaries to accumulate encrypted traffic today for retrospective decryption once quantum capabilities mature, meaning the window for proactive migration has already begun to close. This paper presents a comprehensive, multi-faceted examination of quantum cryptography as the security paradigm required for the post-quantum era. It traces the quantum mechanical principles underlying both the threat and the solution, provides a detailed analysis of the four NIST-standardized post-quantum algorithms (ML-KEM, ML-DSA, SLH-DSA, and HQC), evaluates Quantum Key Distribution as a complementary long-term technology, and examines practical migration strategies, performance trade-offs, and governance frameworks. The research demonstrates that a structured, phased transition to quantum-safe cryptography is both technically feasible and operationally necessary.

Index Terms — quantum cryptography; post-quantum cryptography; quantum key distribution; NIST standards; ML-KEM; ML-DSA; SLH-DSA; HQC; lattice-based cryptography; harvest now decrypt later; Shor's algorithm; cryptographic agility; quantum-safe migration.

I. INTRODUCTION

For more than four decades, the security of digital communications has rested upon the mathematical intractability of two fundamental computational problems: integer factorization and the discrete logarithm problem. The RSA cryptosystem, introduced in 1978, derives its security from the practical impossibility of factoring the product of two large prime numbers using classical computing resources [1]. Elliptic Curve Cryptography (ECC), developed independently by Miller and Koblitz in 1985, exploits the analogous hardness of the elliptic curve discrete logarithm problem to achieve equivalent security with considerably shorter key lengths. These two algorithmic families underpin

Transport Layer Security (TLS), Secure Shell (SSH), digital certificates, and virtually every other protocol responsible for authenticating and encrypting modern internet traffic.

The theoretical foundations of this security regime were challenged in 1994 when Peter Shor demonstrated that a quantum computer operating on a sufficiently large register of quantum bits could factor integers and compute discrete logarithms in polynomial time [2]. Shor's algorithm does not merely improve on classical approaches—it renders the computational problems underlying RSA and ECC tractable, collapsing centuries of projected security into manageable computation. While the quantum computers available in 2025 remain far from the scale required to threaten production cryptographic key sizes, the trajectory of development is unmistakable. IBM, Google, and Microsoft have each demonstrated exponential improvements in qubit count and gate fidelity, and Microsoft's announcement of the Majorana 1 topological qubit chip in February 2025 represents a potentially decisive step toward fault-tolerant operation [8].

Grover's algorithm, developed in 1996, introduces a secondary quantum threat to symmetric encryption by enabling quadratic speedup in searching unsorted databases [6]. Applied to symmetric key search, Grover's algorithm effectively halves the security margin of any symmetric cipher: a 128-bit AES key achieves only approximately 64 bits of quantum security, mandating migration to 256-bit AES for long-term data protection.

The strategic dimension of the quantum threat extends beyond the moment of quantum computer realization. The Harvest Now, Decrypt Later (HNDL) attack paradigm involves systematically collecting and archiving encrypted network traffic in anticipation of future quantum decryption capabilities [3]. The US National Security Agency's CNSA 2.0 advisory reflects this urgency by mandating quantum-safe implementations in all new National Security Systems by January 2027 [3].

The NIST Post-Quantum Cryptography standardization project, initiated in 2016, reached a landmark milestone in August 2024 with the publication of three finalized standards: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) [4]. A fourth algorithm, Hamming Quasi-Cyclic (HQC), was selected as a backup mechanism in March 2025 [10]. Major technology platforms—including Microsoft Windows, Apple iMessage, Google Chrome, and Cloudflare—have already begun integrating these standards into production deployments.

A. Research Objectives

This research pursues five interrelated objectives: (1) to explain the quantum mechanical principles that simultaneously motivate the threat to classical cryptography and enable quantum cryptographic solutions; (2) to provide a comprehensive review of the NIST post-quantum standardization process; (3) to analyze the mathematical structure and performance characteristics of standardized post-quantum algorithms; (4) to examine the practical, organizational, and technical challenges associated with migrating from classical to quantum-resistant cryptographic infrastructure; and (5) to identify priority research areas and make actionable recommendations for practitioners and policymakers.

B. Scope and Significance

The transition from classical to quantum-safe cryptography has been characterized as the most consequential cryptographic infrastructure change since the introduction of public-key cryptography. The US Office of Management and Budget has estimated the cost of transitioning federal systems to post-quantum cryptography at approximately USD 7.1 billion over the period 2025–2035 [5]. This research contributes to the education of future information technology professionals by providing a rigorous, accessible, and current treatment of the quantum cryptography transition.

II. LITERATURE REVIEW

A. The Quantum Threat to Classical Cryptography

Shor's 1994 paper [2] is the foundational reference for the quantum threat to asymmetric cryptography, establishing the polynomial-time factoring algorithm and demonstrating that both RSA and Diffie-Hellman key exchange paradigms

are simultaneously vulnerable. Grover's 1996 contribution [6] addressed symmetric cryptography—while the quadratic speedup is far less catastrophic than Shor's polynomial improvement, its implications are significant: any symmetric cipher or hash function must effectively double its key or output length to maintain equivalent security against a quantum adversary.

Bernstein and Lange [14] conducted a comprehensive survey of post-quantum cryptographic options prior to the NIST standardization effort, cataloguing lattice-based, code-based, hash-based, and multivariate polynomial schemes. The Global Risk Institute's 2024 expert survey found that a majority of respondents assigned at least a 50% probability to a cryptographically relevant quantum computer existing within 15 years [7].

B. Quantum Key Distribution

Bennett and Brassard's 1984 paper introducing the BB84 protocol [9] established the theoretical foundation for Quantum Key Distribution (QKD). Unlike post-quantum cryptography, which achieves quantum resistance through mathematical hardness assumptions, QKD relies on quantum physical principles—the no-cloning theorem and the disturbance introduced by measurement—providing information-theoretic security independent of the eavesdropper's computational resources. Commercial QKD deployments have been demonstrated in China's quantum communication satellite network and in metropolitan fiber networks in Tokyo, Geneva, and Vienna.

C. Post-Quantum Cryptography Standardization

The NIST Post-Quantum Cryptography Standardization Project [4], launched in December 2016, represents the most comprehensive cryptographic evaluation process ever undertaken. From 82 initial submissions, the project proceeded through four rounds of public cryptanalysis. CRYSTALS-Kyber (now ML-KEM under FIPS 203) emerged as the primary key encapsulation mechanism; CRYSTALS-Dilithium (ML-DSA, FIPS 204) and SPHINCS+ (SLH-DSA, FIPS 205) provide digital signature functionality. The March 2025 selection of HQC as a fifth algorithm addresses NIST's goal of maintaining mathematical diversity in the post-quantum portfolio.

D. Industry and Government Responses

The NSA's CNSA 2.0 advisory established binding timelines for US National Security Systems, mandating quantum-safe implementations by January 2027 for newly acquired systems [3]. Microsoft integrated ML-KEM and ML-DSA into SymCrypt, its core cryptographic library, making post-quantum capabilities available across Windows, Azure, and Microsoft 365 [8]. Cloudflare reported that by the end of 2025, over 50% of its traffic was secured with post-quantum key agreement [11].

E. Research Gaps

Despite substantial progress, several important research gaps remain. Performance characterization of PQC algorithms on resource-constrained embedded systems remains an active area. Formal verification of PQC implementations against side-channel and fault-injection attacks is an urgent priority, as multiple implementation-level weaknesses have been identified in early deployments. Standardized frameworks for cryptographic agility at the protocol level and interaction between PQC algorithms and hardware security modules (HSMs) also require further research.

III. METHODOLOGY

A. Research Design

This paper adopts a descriptive-analytical research design grounded in systematic literature review methodology. The approach integrates peer-reviewed academic scholarship with authoritative technical documentation from standards bodies, government agencies, and leading industry organizations to construct a comprehensive and critically evaluated picture of the field.

B. Data Collection

Academic sources were identified through systematic searches of IEEE Xplore, ACM Digital Library, arXiv, MDPI, ScienceDirect, SpringerLink, and Frontiers in Blockchain. Technical standards and policy documents were obtained directly from NIST, the NSA, the UK NCSC, the OMB, and ENISA. Industry research reports were sourced from Microsoft Security, Cloudflare, Google, ISACA, Boston Consulting Group, and the Global Risk Institute. Searches were conducted from January through March 2025, with emphasis on publications from 2020 onward.

C. Analysis Framework

Collected materials were analyzed thematically across five primary dimensions: (1) quantum mechanical principles underlying threat and defense; (2) algorithmic structure and security properties of standardized post-quantum schemes; (3) performance and implementation characteristics across diverse computing environments; (4) practical organizational challenges and transition strategies; and (5) the policy and governance landscape shaping the global response.

D. Limitations

Three principal limitations apply to this research. First, the field is advancing at an unusually rapid pace; hardware milestones and standardization decisions that post-date the literature review window may alter some conclusions. Second, the research draws primarily on English-language sources. Third, as a systematic review, the paper does not generate original experimental data; performance figures cited are drawn from published benchmarking studies.

IV. QUANTUM CRYPTOGRAPHY: PRINCIPLES, STANDARDS, AND TRANSITION

A. Quantum Mechanical Foundations

A rigorous understanding of quantum cryptography requires familiarity with three foundational quantum mechanical phenomena: superposition, entanglement, and quantum interference. Superposition enables quantum computers to process exponentially many computational paths simultaneously. Shor's algorithm exploits superposition to explore all possible factors of a large integer in parallel, then uses quantum interference to amplify the probability of measuring the correct factor [2]. Entanglement establishes correlations between qubits that have no classical analogue, enabling provably secure key distribution in QKD protocols [9]. The no-cloning theorem guarantees that an eavesdropper intercepting a quantum key transmission cannot copy the quantum states without introducing detectable disturbances.

B. Post-Quantum Cryptographic Algorithms: Structure and Security

1) ML-KEM (FIPS 203): Lattice-Based Key Encapsulation

ML-KEM, derived from CRYSTALS-Kyber, is the NIST-standardized algorithm for key encapsulation. Its security rests on the Module Learning With Errors (MLWE) problem. ML-KEM is specified at three security levels targeting approximately 128, 192, and 256 bits of security. At the ML-KEM-768 level, public keys are 1,184 bytes and ciphertexts are 1,088 bytes. Benchmarking on modern hardware demonstrates encapsulation and decapsulation operations completing in microseconds, making ML-KEM suitable for high-throughput TLS handshakes.

2) ML-DSA (FIPS 204): Lattice-Based Digital Signatures

ML-DSA, standardized from CRYSTALS-Dilithium, provides digital signature functionality. Its security rests on the hardness of Module Learning With Errors and Module Short Integer Solution (MSIS). At the ML-DSA-65 security level, public keys are 1,952 bytes and signatures are 3,293 bytes. Performance benchmarks indicate signature generation and verification times on the order of hundreds of microseconds on contemporary processors.

3) SLH-DSA (FIPS 205): Hash-Based Digital Signatures

SLH-DSA, standardized from SPHINCS+, represents the most conservative post-quantum signature scheme. Its security relies exclusively on the collision resistance and preimage resistance of the underlying hash function—properties subject to decades of intense cryptanalytic scrutiny. At the SLH-DSA-SHA2-128s parameter set, signatures

are 7,856 bytes. SLH-DSA is recommended for applications where long-term security assurance is paramount, such as firmware signing and certificate authority operations.

4) HQC: Code-Based Key Encapsulation

Hamming Quasi-Cyclic (HQC), selected by NIST in March 2025 [10], derives its security from the hardness of decoding random linear error-correcting codes—a problem that has resisted quantum attack for nearly five decades. HQC serves as a mathematical backup to ML-KEM with independent security foundations. Its public keys are approximately 4,346 bytes at the 128-bit security level, with relatively fast encapsulation and decapsulation operations.

Table I. Comparison of NIST Post-Quantum Cryptographic Standards

Algorithm	Standard	Type	Security Basis	Public Key	Sig/CT Size
ML-KEM-768	FIPS 203	KEM	MLWE lattice	1184 B	1088 B (CT)
ML-DSA-65	FIPS 204	Signature	MLWE/MSIS	1952 B	3293 B
SLH-DSA-128s	FIPS 205	Signature	Hash functions	32 B	7856 B
HQC-128	NIST Sel.	KEM	Code decoding	4346 B	4497 B (CT)
RSA-2048	(Classical)	KEM/Sig	Integer factoring	256 B	256 B
X25519	(Classical)	KEM	Elliptic curve DLP	32 B	32 B

CT = Ciphertext. Key sizes approximate.

C. The Harvest Now, Decrypt Later Threat

The HNDL threat model demands attention because it decouples the moment of harm from the moment of attacker capability. Intelligence assessments from multiple governments suggest that sophisticated state-level actors have been systematically executing HNDL strategies since at least the early 2010s, accumulating petabytes of encrypted traffic. The NSA's 2022 CNSA 2.0 advisory explicitly acknowledges this threat as the primary rationale for mandating quantum-safe transitions on accelerated timelines [3]. For data with confidentiality requirements extending beyond ten years—government records, financial audit trails, health records, and intellectual property—immediate migration to quantum-safe encryption is the only defensible posture.

D. Migration Strategies and Transition Challenges

The transition from classical to quantum-resistant cryptographic infrastructure touches every layer of the information systems stack: cryptographic libraries, protocol implementations, hardware security modules, certificate authorities, key management systems, network appliances, and application code.

1) Cryptographic Discovery and Inventory

Before migration can begin, organizations must develop a comprehensive inventory of cryptographic assets. Automated cryptographic bill of materials (CBOM) tools are emerging to support this task, parsing codebases, network traffic, and binary executables to identify cryptographic algorithm usage.

2) Hybrid Cryptography

The UK National Cyber Security Centre and multiple standards bodies recommend a hybrid cryptographic approach during the transition period, in which both a classical algorithm (such as X25519) and a post-quantum algorithm (such as ML-KEM) are executed in parallel for each key exchange [3]. Hybrid TLS implementations have been standardized in RFC 8879 and its successors.

3) Cryptographic Agility

Cryptographic agility refers to the architectural property of a system that allows cryptographic algorithms to be replaced without requiring fundamental redesign. Achieving agility in practice requires abstracting cryptographic operations behind configurable interfaces and avoiding hard-coded algorithm assumptions in application logic.

4) Legacy System Challenges

Industrial control systems, avionics, medical devices, and other embedded platforms often have fixed cryptographic implementations. For these systems, the migration path may require hardware replacement or the deployment of cryptographic proxies that handle post-quantum key exchange on behalf of the legacy system.

Table II. Post-Quantum Migration Challenges by System Category

System Category	Primary Challenge	Recommended Approach	Timeline
Web / Cloud Services	TLS certificate/key updates	Hybrid TLS + ML-KEM	2025–2027
Enterprise Software	Library upgrades, API changes	Agile crypto abstraction	2026–2028
IoT / Embedded	Performance, memory limits	HW proxy or replacement	2027–2030
Financial Infrastructure	HSM compatibility	Phased HSM firmware update	2025–2028
Legacy Gov. Systems	Lack of update capability	Crypto proxy / retirement	2027–2032
PKI / CA Infrastructure	Trust anchor replacement	Dual-root hybrid PKI	2025–2027

HSM = Hardware Security Module; PKI = Public Key Infrastructure.

E. Quantum Key Distribution: Complementary Long-Term Technology

The BB84 protocol [9] encodes key bits in the quantum states of individual photons using two non-orthogonal bases. The laws of quantum mechanics guarantee that any measurement not matching the preparation basis collapses the quantum state irreversibly, introducing errors detectable by the communicating parties. Despite its theoretical elegance, QKD faces significant practical deployment barriers: photon loss in optical fiber limits practical QKD range to approximately 100 kilometers without quantum repeaters, satellite-based QKD requires clear line-of-sight, and dedicated quantum channels impose substantial infrastructure costs. The prevailing expert consensus recommends that organizations focus near-term quantum migration efforts on post-quantum cryptography while supporting continued QKD research.

F. Performance Analysis and Implementation Considerations

Benchmarking studies on contemporary server-class hardware indicate that ML-KEM-768 operations complete in approximately 50–100 microseconds, comparable to X25519. ML-DSA-65 signature verification completes in approximately 200 microseconds—acceptable for most use cases. SLH-DSA signature generation requires several milliseconds due to the large number of hash function invocations, making it better suited to offline signing operations.

Resource-constrained environments present more significant challenges, as microcontrollers with limited RAM may struggle to accommodate ML-KEM's key and ciphertext buffers simultaneously.

G. Governance and Policy Frameworks

In the United States, National Security Memorandum 10 (NSM-10) established quantum computing as a national security priority. The Quantum Computing Cybersecurity Preparedness Act, signed in December 2022, requires federal agencies to inventory quantum-vulnerable cryptographic systems and submit migration plans to OMB [5]. Internationally, the EU's NIS2 Directive includes quantum resilience among its security requirements, and ENISA has published a post-quantum cryptography integration study for EU member states. China has pursued an independent post-quantum standardization track through the Chinese Cryptography Standardization Technical Committee.

V. RESULTS AND DISCUSSION

A. State of PQC Adoption

As of early 2025, post-quantum cryptography adoption is concentrated in large technology platforms. Google, Apple, Signal, WhatsApp, and Cloudflare have each deployed ML-KEM in their primary products, providing de facto post-quantum protection to hundreds of millions of users. However, enterprise adoption remains limited: a 2024 ISACA survey found that fewer than 15% of enterprise security teams had initiated formal post-quantum migration planning [12]. The gap between platform-level adoption and enterprise readiness is the most significant near-term vulnerability in the global post-quantum transition.

B. Algorithm Security and Cryptanalytic Developments

To date, no polynomial-time quantum algorithm for Module Learning With Errors—the hardness problem underlying ML-KEM and ML-DSA—has been identified. The best known quantum attacks require exponential quantum resources, providing confidence that the algorithms will remain secure for the foreseeable future. However, the history of cryptography counsels appropriate humility: SIDH/SIKE, a Round 3 finalist, was completely broken by a classical polynomial-time attack in July 2022, underscoring the importance of maintaining algorithmic diversity (as HQC selection reflects) and deploying hybrid schemes for defense-in-depth.

C. Implications for Information Technology Practice

Software developers must audit their applications for use of quantum-vulnerable cryptographic primitives, including RSA, ECDH, ECDSA, and DSA. Security architects designing new systems should follow the principle of cryptographic agility from the ground up, implementing hybrid key exchange where feasible and documenting all cryptographic dependencies in a cryptographic bill of materials. Organizations should prefer configurable cryptographic algorithm selection over hard-coded choices to facilitate future auditing and migration.

VI. FUTURE RESEARCH DIRECTIONS

A. Lightweight Post-Quantum Cryptography

Research into lightweight post-quantum schemes—algorithms optimized for microcontrollers, smart cards, and IoT devices—is an active and important area. Promising directions include structured lattice variants with smaller key sizes, optimized hash-based schemes, and hybrid constructions leveraging hardware acceleration primitives on modern embedded platforms.

B. Quantum Repeaters and Long-Distance QKD

Practical deployment of QKD at intercontinental scale requires quantum repeaters—devices that can extend the range of quantum channels by entanglement swapping without measuring the quantum information. Progress in quantum memory technology, entanglement purification, and fault-tolerant quantum communication would make QKD a viable complement to post-quantum cryptography for the highest-security applications.

C. Formal Verification of PQC Implementations

Several implementation-level side-channel vulnerabilities have been identified in early deployments of lattice-based cryptographic schemes, including timing attacks exploiting data-dependent branching in polynomial multiplication routines. Formal verification methods—including machine-checked proofs of implementation correctness and constant-time execution—are urgently needed for comprehensive coverage of NIST-standardized algorithms.

D. Cryptographic Agility Frameworks

Standardized frameworks for cryptographic agility—specifying how algorithms should be negotiated, parameters communicated, and transitions executed in a coordinated, backward-compatible manner—are needed at the protocol level. Developing agility-aware protocol design patterns and tooling for automated algorithm negotiation is an important research and standardization priority.

VII. CONCLUSION

This paper has provided a comprehensive examination of quantum cryptography as the foundational security paradigm for the post-quantum era. The central conclusion is unambiguous: the quantum threat to classical asymmetric cryptography is neither speculative nor distant in its practical implications. The HNDL attack strategy ensures that the security of sensitive data with long-term confidentiality requirements is already at risk, regardless of when cryptographically relevant quantum computers are realized.

The NIST Post-Quantum Cryptography standardization process has delivered a robust, mathematically diverse portfolio of quantum-resistant algorithms—ML-KEM for key encapsulation, ML-DSA and SLH-DSA for digital signatures, and HQC as a code-based backup—that are ready for immediate deployment. Organizations should immediately initiate cryptographic discovery to identify all uses of quantum-vulnerable algorithms. New system designs should embed cryptographic agility from the outset. Hybrid cryptographic deployments provide defense-in-depth against both unforeseen classical vulnerabilities in new algorithms and continued classical threats. High-value data stores with long-term sensitivity requirements should be re-encrypted with quantum-resistant algorithms as a priority.

In conclusion, the quantum cryptography transition is among the most consequential undertakings in the history of information security. The technical tools are available; the regulatory frameworks are taking shape; the industry is moving. What remains is for every organization that depends on cryptographic security to engage seriously, plan strategically, and act without further delay.

ACKNOWLEDGMENT

The authors gratefully acknowledge the guidance and support of Prof. Roshni Patel, whose mentorship shaped the direction and rigor of this research. Thanks are also extended to the Department of Information Technology for providing access to research resources and to the broader cryptographic research community for the wealth of publicly available scholarly work upon which this paper draws.

REFERENCES

- [1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.
- [2] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. IEEE Symp. Foundations of Computer Science*, Santa Fe, NM, USA, 1994, pp. 124–134.
- [3] National Security Agency, "Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) Cybersecurity Advisory," NSA/CSS, Fort Meade, MD, USA, Tech. Rep., Sep. 2022.
- [4] National Institute of Standards and Technology, "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," NIST, Gaithersburg, MD, USA, Aug. 2024.

- [5] Office of Management and Budget, "Report on Post-Quantum Cryptography," Executive Office of the President, Washington, DC, USA, 2024.
- [6] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proc. 28th Annu. ACM Symp. Theory of Computing, Philadelphia, PA, USA, 1996, pp. 212–219.
- [7] Global Risk Institute, "Expert Survey on the Likelihood of a Quantum Computer Breaking RSA-2048 within 15 Years," Global Risk Institute, Toronto, ON, Canada, Tech. Rep., 2024.
- [8] Microsoft, "Quantum-safe security: Progress towards next-generation cryptography," Microsoft Security Blog, Aug. 2025.
- [9] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175–179.
- [10] National Institute of Standards and Technology, "NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption," NIST, Gaithersburg, MD, USA, Mar. 2025.
- [11] Cloudflare, "State of the post-quantum Internet in 2025," Cloudflare Blog, 2025.
- [12] ISACA, "Post-Quantum Cryptography: A Call to Action," ISACA, Schaumburg, IL, USA, Industry White Paper, 2025.
- [13] L. Chen et al., "Report on Post-Quantum Cryptography," NIST Internal Report 8105, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2016.
- [14] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, Sep. 2017.
- [15] A. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.
- [16] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, no. 6, pp. 1–40, Sep. 2009.
- [17] NIST, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," FIPS 203, National Institute of Standards and Technology, Gaithersburg, MD, USA, Aug. 2024.
- [18] NIST, "Module-Lattice-Based Digital Signature Standard," FIPS 204, National Institute of Standards and Technology, Gaithersburg, MD, USA, Aug. 2024.
- [19] NIST, "Stateless Hash-Based Digital Signature Standard," FIPS 205, National Institute of Standards and Technology, Gaithersburg, MD, USA, Aug. 2024.
- [20] European Union Agency for Cybersecurity (ENISA), "Post-Quantum Cryptography: Current State and Quantum Mitigation," ENISA, Heraklion, Greece, Tech. Rep., 2021.